REMARKS

This Amendment is fully responsive to the non-final Office Action dated March 30, 2009, issued in connection with the above-identified application. Claims 1, 2, 4, 5 and 10-12 are pending in the present application. With this Amendment, claims 1, 2, 11 and 12 have been amended, claim 4 has been canceled without prejudice or disclaimer to the subject matter therein, and claims 14-17 have been added. No new matter has been introduced by the amendments made to the claims, or by the new claims added. Favorable reconsideration is respectfully requested.

In the Office Action, claims 1, 2, 11 and 12 have been objected to because of the misuse of labels in the claims. Specifically, the Examiner alleges that the claims use labels (i), (ii) and (iii) to define two steps. However, the Applicants respectfully point out that the labels (i), (ii) and (iii) used in claim 1 define respectively three different steps performed by the first device and the second device recited in the claim.

In other words, each of the devices (i.e., first and second devices) recited in claim 1 perform three primary steps, which are indicated by labels (i), (ii) and (iii). The use of the labels is meant to clearly set out the different steps being performed by the devices, thereby clarifying the scope of the claims. Additionally, there should be no confusion caused by the use of the labels given that the labels (i.e., (i), (ii) and (iii)) are not referenced by any other claims.

Also, the Applicants respectfully point out that claims 2, 11 and 12 do not use the labels (i), (ii) and (iii). Accordingly, withdrawal of the objection to claims 1, 2, 11 and 12 is now respectfully requested.

In the Office Action, claim 1 has been rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Specifically, the Examiner asserts that the limitation "the communication device" lacks sufficient antecedent basis. The Applicants have amended claim 1 to replace the limitation "the communication device" with the limitation "the first device." Accordingly, withdrawal of the rejection to claim 1 under 35 U.S.C. 112, second paragraph, is respectfully requested.

In the Office Action, claims 1, 2, 5, 10, 11 and 12 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie et al. (U.S. Patent No. 5, 371,794, hereafter "Diffie") in

view of Bellare et al. (article entitled "Keying Hash Functions for Message Authentication," 1996, hereafter "Bellare"); and claim 4 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie and Bellare, and further in view of Morais et al. (U.S. Publication No. 2003/0093669, hereafter "Morais").

Independent claims 1, 2, 11 and 12 have been amended to include the limitations of dependent claim 4, and claim 4 has been canceled. The Applicants assert that independent claims 1, 2, 11 and 12 (as amended) are clearly distinguished from the cited prior art noted above. Claim 1 (as amended) recites the following features:

"[a]n encrypted communication system comprising a first device and a second device, wherein

the first device (i) encrypts a first key using a public key of the second device to generate first encrypted data, and transmits the first encrypted data to the second device, (ii) receives second encrypted data from the second device, the second encrypted data being generated by encrypting a third key of the second device using a public key of the first device at the second device, and decrypts the second encrypted data using a secret key of the first device to obtain a second key, and (iii) generates, based on the first and second keys, a first encryption key for use in communication with the second device,

the second device (i) encrypts the third key using the public key of the first device to generate the second encrypted data, and transmits the second encrypted data to the first device, (ii) receives the first encrypted data from the first device, and decrypts the first encrypted data using a secret key of the second device to obtain a fourth key, and (iii) generates, based on the third and fourth keys, a second encryption key for use in communication with the first device, and

the first and second devices perform encrypted communication using the first and second encryption keys,

wherein the first device concatenates the first and second keys to generate concatenated data, calculates a hash value for the concatenated data, generates the first encryption key and a first hash key based on the hash value for the concatenated data, calculates using the first hash key a first hash value for the first transmission data, encrypts the first transmission data using the

first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, the first encryption key being distinct from the first hash key,

wherein the second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the first device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data to generate decrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the decrypted first transmission data is not tampered with when the received first hash value matched the calculated second hash value, the second encryption key being distinct from the second hash key."

The features noted above in independent claim 1 are similarly recited in independent claims 2, 11 and 12 (as amended). Additionally, the features noted above in independent claim 1 (and similarly recited in independent claims 2, 11 and 12) are not believed to be disclosed or suggested by the cited prior art.

Diffie does not disclose the use of a hash function, and naturally, neither discloses nor suggests creating a first hash key with a high reliability. And, Bellare merely mentions use of two keys kl and k2 (4.1 lines 1-3), and does not disclose that the first device uses different keys separately existing in the first and second devices.

Moreover, although the Examiner rejects claim 4 (now incorporated into amended claim 1, 2, 11 and 12) based on ¶[0052] of Morais, the Applicant assert that independent claims 1, 2, 11 and 12 (as amended) are distinguishable over Morais for at least the reasons noted below.

Morais in ¶[0052] merely discloses a signature and does not disclose the use of a hash function. Also, the signature according to Morais and the hash key according to the present application are different.

Finally, the technique for creating the signature in Morais is different from the technique of creating the first hash key in the present invention. In the present invention, the process of creating the first hash value with use of the first hash key cannot be realized by Morais (e.g., with use of the data disclosed in ¶[0052]).

The first device of the present application creates the first key based on different keys which separately exist in the first and second devices. Thus, even if the content held by one of the devices (e.g., the first device) is disclosed to a third party, the reliability of the communication system is ensured unless the content held by the other one of the devices (e.g., the second device) is also disclosed to the third party.

Therefore, the Applicants assert that even if one of ordinary skill in the art combined the teaching of Diffie, Bellare and Morais (as suggested by the Examiner), the combination still fails to arrive at the present invention (as recited in independent claims 1, 2, 11 and 12).

Accordingly, no combination of Diffie, Bellare and Morais would result in, or otherwise render obvious, independent claims 1, 2, 11 and 12 (as amended). Likewise, no combination of Diffie, Bellare and Morais would result in, or otherwise render obvious, claims 5, 10 and 14-17 at least by virtue of their respective dependencies from independent claims 1, 2, 11 and 12.

In light of the above, the Applicants respectfully submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner withdraw the rejections presented in the outstanding Office Action, and pass the present application to issue.

The Examiner is invited to contact the undersigned attorney by telephone to resolve any remaining issues.

Respectfully submitted,

Yuichi FUTA et al.

/Mark D. Pratt/
2009.06.29 13:10:37 -04'00'

By: Mark D. Pratt
Registration No. 45,794
Attorney for Applicants

MDP/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
June 29, 2009